Email message, dated May 20, 2005, 3:18 p.m., to General Services, Budget Office, Energy Office, Materials Management Office, and General Counsel

What is phishing?   "*Phishing* is a technique used to gain personal information for purposes of identity theft, using fraudulent e-mail messages that appear to come from legitimate businesses. These authentic-looking messages are designed to fool recipients into divulging personal data such as account numbers and passwords, credit card numbers and Social Security numbers. (Source: http://www.computerworld.com/securitytopics/security/story/0,10801,89096,00.html).

"Phishing" attacks are named so because the senders are "fishing" for recipients' personal information..." Source: (http://en.wikipedia.org/wiki/Phishing) For an example of phishing, see: http://dc.internet.com/news/article.php/2238431

Consider this information from *The Dangers of phishing*, InfoWorld, Jan 24, 2005:
1. "Nearly 5% of recipients respond to phishing--a far greater rate than the less than 1% who respond to everyday spam."
2. "Security experts expect the problem to get worse in 2005.
3. "Because phishing is a main artery for identity theft... it's expected to spur more hacking attempts against" datacenters.
4. If users choose their own passwords, it's likely they use the same passwords (or PIN) in many places. Once that password or PIN is known by a successful phisher, many databases can now be scoured to look for exact or similar username/password situations.

When you receive unsolicited emails........
1. Be extremely cautious in clicking on a link that is provided in an email you receive. When you click on it, it could actually take you somewhere other than where you *think* you're going. Be especially concerned about an address containing the "@" symbol (e.g., http://www.google.com@additional.com/). The same is true for misspelled URLs or subdomains; for example, http://www.yourfavbankdomain.com.spamdomain.net (note the ".com" followed by a ".net") or http://www.wochovia.com (notice how Wachovia is misspelled).
2. Along those lines, in GroupWise, you can check to see if the URL you are looking at is actually the URL that you will go to when you click on it. Do the following:
    a. Place your mouse arrow over the URL address given in the email
    b. RIGHT click. At the bottom of the new window displayed, it may show the address there.
    c. If you don't see the address there, then LEFT click on the word "Properties" to see what the URL is.   If the URL there doesn't match the one displayed to you in the email, you most definitely do not want to go there.
3. If the language in the email seems odd, it's likely to be phishing by people who typically don't speak English.
4. The FTC warns users to be suspicious of any official-looking e-mail message that asks for updates on personal or financial information and urges recipients to go directly to the Web site of the company to find out whether the request is legitimate. If you suspect you have been phished, forward the e-mail to uce@ftc.gov or call the FTC help line, 1-877-FTC-HELP. For additional information on reporting such crimes or suspicians, see http://www.congressionalfcu.org/aboutus/securitycenter/Warning%20Against%20Fraudulent%20E-Mail%20Schemes.pdf.
5. Don't give out personal data such as passwords over the Internet.
6. Don't give out bank account or credit card information over the Internet in response to a questionnaire. The only time you should be giving out such information is when making a purchase.

Questions? Give anyone in IS a call!

Information Services